



Service

**General Services Administration
Technology Transformation**

**1800 F Street NW
Washington, D.C. 20006**

Crowdsourced Security and Penetration Testing

GSA Project Number XXXXXX

**In Support of
General Services Administration (GSA) Technology Transformation Service (TTS)**

**Administered by
General Services Administration
National Capital Region**

TABLE OF CONTENTS

| | |
|-------------------------|---|
| Introduction/Background | 3 |
| Scope of Work | 4 |
| Period of Performance | 5 |
| Place of Performance | 5 |
| Solution Requirements | 5 |
| Schedule/Milestones | 6 |
| Acceptance Criteria | 6 |
| Other Requirements | 7 |

INTRODUCTION

This document represents a Statement of Work (SOW) to acquire Crowdsourced Security & Penetration Testing services using vetted crowd members for the General Services Administration (GSA), Technology Transformation Service (GSA TTS) Login.Gov Program.

Background

GSA TTS is designing and developing a Shared Authentication Platform to answer and meet recent federal directives and action plans released by the Executive Office of the President to provide citizens with secure singular digital accounts that can be used government-wide to access participating federal agencies. Congress saw the need for citizens to securely access federal agencies and passed the Cybersecurity Act (CISA) in October 2015 to strengthen the Nation's Cybersecurity. The Executive Office of the President defined actions federal agencies can follow to meet CISA in the Cybersecurity National Action Plan in February 2016.

Armed with knowledge gained from an initial operational capability utilizing third-party credentials and with valuable Government, industry, and customer input, GSA TTS will operationalize a shared authentication platform titled Login.gov that provides citizens with government-provided digital identities established at National Institute of Standards and Technology (NIST) Level of Assurance LOA1 and LOA3 in 800-63-2 with remote proofing, in a simple, elegant manner from a technical environment that is built on experiences, processes, and infrastructure that will use the latest available technology to safeguard all user data.

Objectives

The Government intends to award one contract to the offeror who can supply to GSA TTS with "Crowdsourced Security and Penetration Testing Services"

Scope

GSA has an immediate need to perform penetration testing and web application assessment against Login.gov, a Software as a Service (SaaS) federated single sign-on solution that provides and supports simple and secure access to public-facing consumer services and information with mandatory use of two-factor authentication, while protecting consumer privacy. The solution is targeted to the public to allow citizens to more easily interact with their government using a single sign on account. The service is expected to support millions if not tens of millions of americans and to do so will store their Personally Identifiable Information (PII). The system is expected to be widely targeted by attackers.

GSA requires Crowdsourced Security and Penetration Testing service that mimics attacks and detects the security flaws that real-world hackers use to breach the Login.gov platform.

This requirement is one in a series of security assessment requirements for login.gov, commonly known as penetration testing. In this instance, the service is seeking a vendor with crowdsourced

vulnerability discovery capabilities using penetration testing methods and disclosure programs for large enterprises. The selected vendor will attempt to compromise the service in real-time, with pre-determined monitoring and safeguards in place. This is planned to begin after login.gov has added up to 500 users to the service who require NIST Level of Assurance 3 (LOA3) security. These users are unique as they will be the first users to input personally identifiable information (PII) into login.gov. This red team exercise is designed to test the service at a higher level of assurance, NIST LOA3, than other login.gov users.

This red team exercise is an important security step necessary to achieve authority to operate (ATO) login.gov at this higher level of assurance.

Further, GSA requires the winning vendor to perform background checks to verify the integrity of the individuals performing the test in order to increase confidence that all identified findings will be disclosed. Furthermore, all disclosures should include comprehensive vulnerability triage, validation, and manual reproduction of identified vulnerabilities.

SCOPE OF WORK

GSA requires the following products and services:

Crowdsourced Security & Penetration Testing focusing on the Login.gov platform running in Amazon Web Services using a pre-vetted and private pool of researches. Assessment will focus on both LOA1 and LOA3 integrations.

- Currently login.gov's code repository contains 50,000 lines of code
- At the time of testing login.gov will have 500 or more active LOA1 users and 500 active LOA3 users.

Test accounts will be available for each researcher. The assessment shall have the following required objectives:

Core Objectives

1. Target/attack Relying Party integrations and associated users, and user data; testing both SAML certs and OIDC tokens.
2. Target/attack Login.gov web servers, rooting, and vulnerability to data exfiltration.
3. Target/attack third party vulnerabilities in third party integrations. Penetration testing of 3rd party platforms is out-of-scope however the "integration" of Login.gov with a 3rd party platform via APIs is in scope.
4. Target/attack of Login.gov via public code repo available at Github.com and/or DevOps chain.
5. Traditional web application penetration test such as OWASP etc.

Bonus Objectives (IF web servers are compromised/rooted)

1. Target/attack of encryption implementation and possible cracking of encryption implementation - in transit and at rest.

PERIOD OF PERFORMANCE

The period of performance should be as follows 2-4 weeks of scoping, followed by a 4-6 week window for the penetration test (with the test itself happening within a 2-3 week period inside that window). The engagement timeframe will be mutually agreed to after consultation between the Government and the vendor.

PLACE OF PERFORMANCE

Crowdsourced Security & Penetration Testing is a remote penetration testing product service, regular access to government facilities is not required.

SOLUTION REQUIREMENTS

1. Solution must utilize a secure web gateway with API access for all reportable crowd findings and must be hosted by the contractor.
2. Secure web gateway must implement Two-Factor Authentication (2FA).
3. Crowd members must be required to VPN to the secure web gateway for all assessment activities.
4. The VPN gateway must perform Full Packet Capture of all crowd activities during the assessment so that there is an audit trail of researcher activity.
5. All crowd members must be vetted by the contractor, in accordance to the agreed upon crowd criteria, prior to the crowd members being invited to the assessment.
6. Crowd member vetting must include the following or equivalent; Video Interview, Identity Verification, Background Investigation, Written and Practical Skills assessments.
7. All crowd members shall be under Non-Disclosure Agreement (NDA) with the contractor and agree that all findings from assessment activities for assets within scope under the agreed upon contract are solely owned by the US Government.
8. Contractor is responsible for all researcher management to include determining value of crowd payments and the actual payment to the crowd members for discoveries.
9. Solution must have predetermined IP addresses for all assessment traffic to ensure differentiation between assessment traffic and possible malicious traffic.
10. Contractor must perform each of the following functions without the use of a third party; Triage, Validation and De-duplication of crowd submissions to ensure only high-fidelity reports are provided.
11. Contract shall be Firm-Fixed-Priced based on the scope of each engagement.
12. Contractor must have at least two (2) years proven experience providing crowdsourced vulnerability discovery and disclosure programs for large enterprises.
13. Contractor must be capable of adhering to ISO 29147 and ISO 30111.
14. Contractor must be capable of ensuring that all researchers are U.S. persons or other approved nationalities; are not felons; are not known terrorists, or an associate of a known terrorist or terrorist organization; are not listed on the U.S. Department of Treasury's Specially Designated Nationals List; or otherwise ineligible to conduct work for the government and have passed criminal background checks performed by the contractor.
15. Solution must utilize Common Vulnerability Scoring System (CVSS) for all vulnerability

submissions

16. For web application assessments, the contractor solution shall provide a visible network map that identifies the extent to which the crowd viewed the web application and must provide clear classification of attacks attempted at locations within the system where applicable.
17. Contractor solution must support customizable reporting by methods such as email, dashboard in formats including but not limited to PDF.

SCHEDULE/MILESTONES

The following are the schedule / milestones for this procurement:

- The engagement timeframe will be mutually agreed to after consultation between the Government and the vendor. During this time, GSA will ensure vendor has accounts setup for all in scope researchers for both an LOA1 and LOA3 integration.
- Vendor shall provide access to the platform for all GSA requested accounts within 7 days of contract award and before the start of penetration testing.

ACCEPTANCE CRITERIA

Acceptance will be contingent on the vendor providing the services including the assessment Core objectives noted above.